Examiner is referring to in section 3 should be "the Appeal Brief filed in January", not the Appeal Brief (Substitute) filed by fax on Feb 19, 2003" as the latter has no argument as to patentability of those limitations of the claim 1 in the Appeal Appendix.

The Examiner is respectfully requested to clarify this because a US court may determine scope of claims basing on applicant's argument successfully in overcoming a rejection, when considering infringement case.

Submitted herewith is a sheet of drawing for FIG 1 & 2, as required by the Examiner in P.4, section 9 & 10. I hereby state that the FIG 1 & 2 submitted are the same as those of the parent application 08/587,448 and no new matter is introduced thereby into the present application.

Respectfully submitted,

Ho Keung, Tse.

Status of Claims :

22 claims are presented. Claims 1, 7, 10, 12, 14, 16, 18, 20, 21, 22 are independent.

Claims 2, 4-6 depends directly or indirectly on independent claim 1.

Claims 8, 9 depend directly on independent claim 7.

Claims 3, 13, 17 depend directly on independent claim 12.

Claim 15 depends directly on independent claim 14.

Amendments to Description:

In the description, P.7, item 4, second paragraph, lines 4-6 that "In the initialization process, the central program sends to the central computer, as mentioned herein above in **item 2**, an **unencrypted** identity of the rightful user of the central program", the term **"unencrypted"** therein is **a typographical error** and the correct term should be "encrypted".

Evidence can be found in **item 2** of the description(P.5), it is disclosed a "Sub-program for providing an Encrypted Identity (EI sub-program)", in which unencrypted identity or its equivalent is not being mentioned.

The replacement paragraph is as follows :

Specifically, when the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an ~~unencrypted~~ encrypted identity of the rightful user of the central program, then the AC sub-program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described herein above in item 3i, if the rightful user has a valid account which is not closed.

Amendments to Claims:

Claim 1 (currently amended) A method for protecting publicly distributed software from unauthorised use, comprising the steps of:

determining if identity ~~means/~~ information, is existing in a processing apparatus ;

using a ~~favourable~~ positive result of said determination as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein :

said identity ~~means/~~ information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity ~~means/~~ information being specific to said rightful user(s) ~~and said software desired to be protected being licensed to said rightful user(s)~~ .

Claim 2 (currently amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

U' cont

authenticating said identity ~~means/~~ information ;

determining said identity ~~means/~~ information as existing, if ~~the result of said authentication is favourable~~ said identity information being authentic and as not existing if otherwise .

Claim ~~6~~ 12 (currently amended) A method for protecting software from unauthorised use , as claimed in claim ~~12~~ 11, wherein said software desired to be protected being first software used on said processing apparatus for determining third information related to hardware and/or software of said processing apparatus ;

wherein further comprising second software for, when being executed, authenticating the identity of the computer on which said second software runs as being said processing apparatus, basing on at least a part of said third information;

and for providing user access to third software if ~~said authentication result is favourable~~ said computer has an authentic identity.

Claim ~~4~~ 3 (currently amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user(s) , for obtaining a service/product.

U1 con't

Claim ~~5~~ 4 (previously amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

Claim ~~6~~ 5 (currently amended) A method for protecting software from unauthorised use, as claimed in claim ~~5~~ 4, wherein further comprising the steps of:

U' con't

~~said processing apparatus having~~ storing an encrypted identity of ~~its rightful~~ a user in said processing apparatus ; and if ~~one~~ all of said protected programs stored in said processing apparatus has a valid user identity which being ~~not~~ consistent with the decryption result of said stored encrypted identity ~~of said processing apparatus~~, permitting use of said protected programs ~~will not be permitted~~ and ~~will be permitted~~ not permitting if otherwise .

Claim ~~7~~ 6 (currently amended) A computer software product for protecting software publicly and individually distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium having said identity program code and said authorising software ;

wherein :

said identity program code and said authorising software are ~~contained~~ stored in said ~~software product~~ medium in such a manner that said authorising software is prevented from being copied therefrom individually; and

U' cont

the improvement resides in said protection basing on no hardware and/or software specific to said rightful user(s) other than said identity program code and said identity program code being specific to said rightful user(s) .

~~and said identity program code and said authorising software existing in a computer readable medium~~ .

Claim ~~8~~ 7 (previously amended) A computer software product as claimed in claim ~~7~~ 6, wherein said operation being operation related to making payment from an account of said rightful user(s) .

Claim ~~9~~ 8 (currently amended) A computer software product as claimed in claim ~~7~~ 6, wherein said authorising software contains said identity program code therein ~~and said computer readable medium being data signal embodied in a carrier wave~~.

Claim ~~10~~ 9 (currently amended) A computer software product for protecting other software against unauthorised use , comprising :

authorising program for, when being executed on a processing apparatus, providing user access to said software desired to be protected ;

U' cont

a computer readable medium having said authorising program ;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program as a part thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof, and access to said software desired to be protected is being provided without causing a said operation being performed.

~~said authorising program existing in a computer readable medium~~

Claim ~~11~~ 10 (currently amended) A computer software product as claimed in claim ~~10~~ 9, wherein said operation being operation related to making payment from an

20

account of said rightful user(s) ~~and said computer readable medium being data signal embodied in a carrier wave~~.

U cont

11 //

Claim ~~12~~ 11 (currently amended) A method for protecting publicly distributed software from unauthorised use , comprising the steps of :

obtaining ~~a~~ first information from a user of a processing apparatus having an identity software ~~/means~~;

using said first information received being correct as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected;

wherein:

said identity software ~~/means~~ being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ; and said second information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed.

U' cont

Claim 13 (previously amended) A method for protecting software from unauthorised use, as claimed in claim ~~12~~ 11, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

Claim 14 (currently amended) A method for protecting publicly distributed software from unauthorised use , comprising the steps of :

U! cont

authenticating identity information ~~/means~~ associated with a processing apparatus ;

using a ~~favourable~~ positive result of said authentication as a pre-condition for causing said processing apparatus to provide user access to said software desired to be protected ;

wherein said identity information ~~/means~~ existing in such a manner that said identity information ~~/means~~ being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information ~~/means~~ being specific to said rightful user(s) ~~and said software desired to be protected being licensed to said rightful user(s)~~.

Claim 15 (previously amended) A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

U' cont

Claim 16 (currently amended) A method for protecting software from unauthorised use , comprising the steps of :

(a) obtaining by protection software running on a processing apparatus, say, first processing apparatus, first information from the user thereof ;

(b) determining by said protection software, from said processing apparatus second information related to the hardware or/and software thereof for future reference in step (c) below, in response to said first information obtained being consistent with third information contained in said protection software ; thereafter

(c) authenticating a processing apparatus, say, second processing apparatus , basing on at least a part of said second information ;

(d) using a ~~favourable~~ positive result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus ;

wherein said third information being confidential information of a rightful user of said software desire to be protected and being necessary for enabling electronic commerce transaction(s) for which said rightful user has to be responsible ; and said method is being performed without causing a said transaction take place .

24

Claim 17 (previously amended) A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

U' cont

Claim 18 (currently amended) A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being ~~obtained~~ communicated to said remote electronic transaction system from said processing apparatus ;

(c) using a ~~favourable~~ positive result of said verification as a pre-condition for ~~determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter~~

~~(d) authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said~~

~~hardware or/and software ;~~

~~(e) using a favourable result of said authentication as a pre-condition for~~ permitting use of said software on said ~~second~~ first processing apparatus ~~, with no charge~~ ;

U' con't

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, ~~third~~ second processing apparatus , without re-charging from said account said cost .

Claim 19 (currently amended) A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge ~~by said software distribution system~~ for repeating ~~at least~~ said sub-method ~~steps c) to e)~~ .

26

Claim 20 (currently amended) A method for protecting software, ~~publicly distributed through a communications network,~~ for use by a user, from unauthorised use ; comprising a sub-method ;

U' con't

wherein said sub-method a protection software being used and "the presence of identity information ~~/means~~ in a processing apparatus" is being used in the creation of said protection software as ~~a~~ an "installation" pre-condition for said protection software to perform in said processing apparatus step (a) below ; and said identity information ~~/means~~ being specific to said user and capable of being used in enabling electronic commerce operation(s) for which said user has to be responsible ;

said sub-method comprising the steps of :

(a) determining by said protection software running on a processing apparatus, say, first processing apparatus with said "installation" precondition being met, first information related to the hardware or/and software of said first processing apparatus, for future reference in step (c) below ; thereafter

(b) determining from a processing apparatus, say, second processing apparatus, second information related to the hardware or/and software thereof;

(c) determining if said second information is consistent with said first information ;

21' cont

(d) using a ~~favourable~~ positive result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on said second processing apparatus, with said "installation" pre-condition not being met ;

thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus, without causing **any** user responsible operation(s) being performed therefor and with no step relating to a new user payment therefor .

Claim 21 (currently amended) A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

U'
cont

~~a)~~ receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

~~b)~~ verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

~~c)~~ using by said data processing apparatus, a ~~favourable~~ positive result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said ~~steps a) to c) are~~ method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

22. (currently amended) A software product comprising a computer readable medium having computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21.

~~said computer code existing in a computer readable medium~~

24